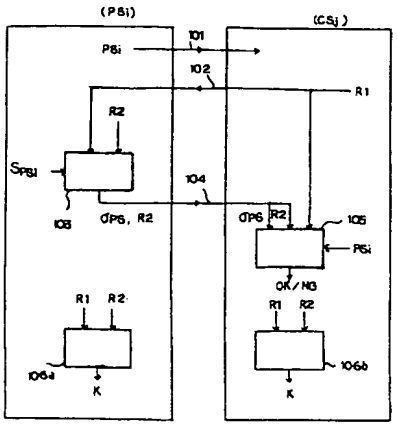
(54) COMMUNICATION METHOD F[illegible]RADIO COMMUNICATION SYSTEM
(11) 5-347617 (A) (43) 27.12.199[illegible]) JP
(21) Appl. No. 4-154779 (22) 15.6.1992
(71) TOSHIBA CORP (72) ATSUSHI SHINPO(3)
(51) Int. Cl⁵. H04L9/06,H04L9/14,H04K1/00

PURPOSE: To reduce the communication quantity by devising the method such that an authentification section authenticates only a radio terminal and a ciphering key between a base station and the radio terminal is shared in common.

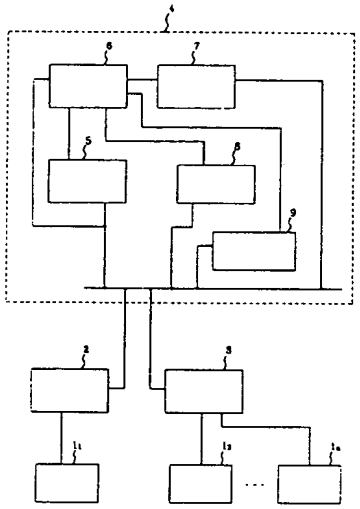
CONSTITUTION: A radio terminal sends an authentication number PSi to a base station and the base station generates a random number R1 and sends it to the radio terminal. The radio terminal receives it to generate a random number R2, an authentication information generating means 103 synthesizes the numbers R1, R2 and secret information Sppi to obtain an authentication number σps and it is sent to the base station together with the random number R2. The random numbers R1, R2, the authentication number PSi and the authentication number σps are given to an authentication information check means 105, which authenticates the radio terminal as the terminal having the PSi when the result of check is OK, ad the radio terminal and the base station generate a common ciphering key by common share means 106a, 106b. Thus, a random number required for mutual authentication consists of key common share information and a function in the device to reduce number of random numbers to be converted thereby reducing the communication quantity.



(54) STORAGE COMMUNICATION PROCESSING UNIT
(11) 5-347618 (A) (43) 27.12.1993 (19) JP
(21) Appl. No. 4-155332 (22) 15.6.1992
(71) NIPPON TELEGR & TELEPH CORP <NTT>
(72) TOMOYOSHI HANEDA(1)
(51) Int. Cl⁵. H04L12/18,H04L12/54,H04L12/58

PURPOSE: To prevent the communication cost from being increased by not extending a line hold time to receive the communication result even when number of destinations of a multiple address call is increased.

CONSTITUTION: A destination number management equipment 6 stores a destination number corresponding to a call identification number given to a multiple address communication call by a call identification number provision device 5, stores the communication result to each destination number, and a communication information storage device 7 stores the communication information subject to multiple address communication. After the communication of the communication information is finished to destination information input output terminal equipments l_2, l_3,-, l_n, a communication result notice equipment 8 informs each destination number divided by each predetermined communication result to the information input output terminal equipment l_1 of a multiple address communication sender. Moreover, when the noticed call identification number is inputted from the sender, an individual communication result notice equipment informs each destination number corresponding to the call identification number and the communication result to each destination number to the sender.

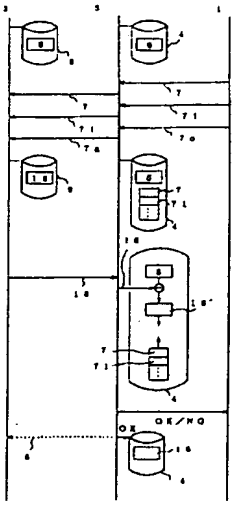


2,3: exchange, 4: store and forward communication processing unit, 9: individual communication result notice equipment

(54) SETTING INFORMATION MANAGEMENT SYSTEM IN TRANSMITTER REMOTE CONTROL SYSTEM
(11) 5-347619 (A) (43) 27.12.1993 (19) JP
(21) Appl. No. 4-155517 (22) 16.6.1992
(71) NEC CORP (72) DAISUKE TANIGUCHI
(51) Int. Cl⁵. H04L12/24,H04L12/26,H04M3/00

PURPOSE: To obtain the setting information management system in the transmitter remote control system in which the operability is not deteriorated even by a line setting revision instruction caused frequently.

CONSTITUTION: A line setting revision instruction of a transmitter 2 instructed from a network management system 1 by the operator is informed to the transmitter 2 from a transmitter control section 3 continuously for a prescribed time and revision setting information is stored in a data base 4. Then revision line setting information 16 being the entire information is read from the transmitter 2 after a lapse of a prescribed time, line setting information 5 before the continuous revision instruction, stored revision setting information 7 and the read revision line setting information 16 are compared to confirm whether or not the setting is correctly implemented. Thus, even in the case of the revision request caused frequently, the turnaround time is reduced and the deterioration in the operability is prevented.



a: in the case of dissidence

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－347617

(43)公開日　平成5年(1993)12月27日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/06					
	9/14					
Ｈ０４Ｋ	1/00	Ｚ	7117－5Ｋ			
			7117－5Ｋ	Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数1（全 18 頁）

(21)出願番号　特願平4－154779

(22)出願日　平成4年(1992)6月15日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　新保　淳
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内

(72)発明者　尾林　秀一
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内

(72)発明者　鶴見　博史
神奈川県川崎市幸区小向東芝町1番地　株式会社東芝総合研究所内

(74)代理人　弁理士　須山　佐一

最終頁に続く

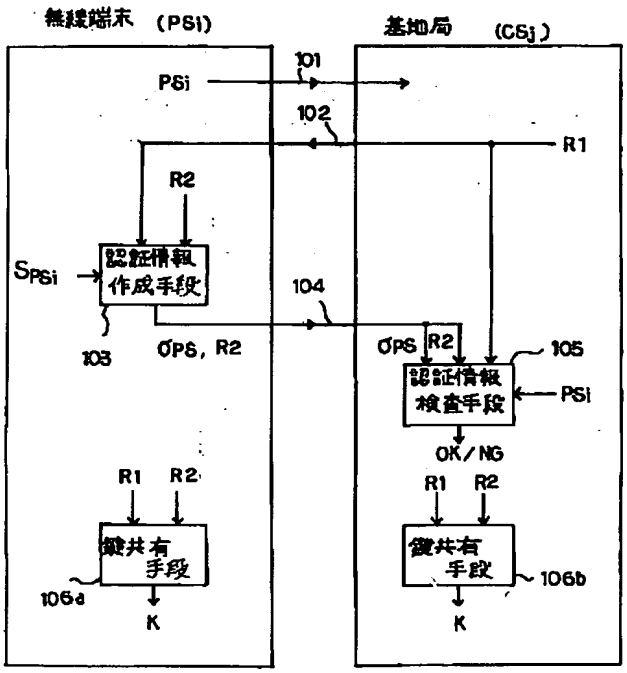
(54)【発明の名称】　無線通信システムの通信方法

(57)【要約】

【目的】　無線通信システムにおける無線端末の認証と基地局と無線端末間の暗号鍵の共有を通信量少なく実現することを目的とする。

【構成】　認証に必要な乱数情報を鍵共有情報として共用する。さらに、ランダム関数を用意し、この出力を乱数として扱うことにより、乱数情報の通信を減らす。

【効果】　鍵共有のために余分な通信がないこと、交換する乱数情報の数が減ることから通信量が少なくなる。



1

【特許請求の範囲】

【請求項１】　複数の無線端末と該無線端末からの通信情報を伝送・交換するネットワーク側装置としての複数の基地局および制御局から構成され、各無線端末は装置固有の第１の秘密情報と基地局の公開情報を有し、前記各基地局は、基地局の第２の秘密情報を有する無線通信システムであって、

前記基地局が第１の乱数を生成して前記無線端末に送信する工程と、

前記無線端末が第２の乱数を生成し、基地局の公開情報を用いて変換することにより鍵配送情報を生成し、前記第１の乱数と前記鍵配送情報と前記第１の秘密情報から認証情報を生成して鍵配送情報と認証情報を前記基地局に送信する工程と、

前記基地局が、前記第１の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認する工程と、

前記基地局が前記第１の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認すると、前記無線端末が前記第２の乱数と前記システムの公開情報から暗号鍵を求める工程と、

前記基地局が、鍵配送情報と基地局の秘密情報から暗号鍵を求める工程と、を具備し、

前記基地局が前記無線端末の正当性を確認することを特徴とする無線通信システムの通信方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、端末の認証および通信内容の暗号化を要する自動車電話や携帯電話などの無線通信システムの通信方法に関する。

【０００２】

【従来の技術】無線通信システムにおいては、有線系のシステムに比べ、通話内容の盗聴及び不正アクセスといった行為が容易となるため、これらを防止するためのセキュリティ対策が重要となる。具体的には、情報チャネルの暗号化及び無線端末の正当性の確認を行う必要が生じる。

【０００３】このような無線通信システムのセキュリティを実現する方式は、次の点を満たすことが望ましい。

【０００４】（１）無線端末の正当性の確認および基地局との間の無線回線の秘匿に必要な暗号鍵の共有のために必要な通信量が少ないこと。

【０００５】（２）無線端末の正当性の確認は、基地局と無線端末の間のみで実行でき、かつ全無線端末に対応した情報を格納するデータベースは制御局に持たせ、基地局にはデータベースを置かないこと。

【０００６】一般に認証や鍵共有のために伝送される情報は１ビットの誤りも許されない場合が多い。一方、基地局と無線端末の間の伝送路は無線回線であるため、誤り率が大きい。誤り訂正符号の利用や誤り検出と再送手順の組み合わせなどにより伝送路の誤り率を低くすることはできるが、一般に許容誤り率を小さく抑えることにより、伝送路のスループットが低下し、通話開始までに時間を要する。従って、認証や鍵共有のために伝送される情報は極力少なくする必要がある。これが（１）の要求項目である。

2

【０００７】（２）は、発呼、着呼の度に生じる認証手順を簡略化する目的で必要となる。発呼、着呼の度に無線端末を認証するために制御局へのアクセスを必要とするのでは制御局への負荷の集中といった問題が生じる。一方、無線端末のデータベースを基地局に持たせる解決法が考えられるが、この場合には基地局の装置規模が大きくなることや基地局のデータベースの一貫性を保つために制御が複雑化することなどの問題が生じる。

【０００８】さらに、将来、マイクロ・セル方式などによる基地局の小型化・セルの小ゾーン化が一層進み、多数の基地局が街頭に設置された状況を想定すると、基地局に対する物理的な攻撃も考慮する必要が生じる。物理的な攻撃とは、例えば、基地局の盗難・分解による基地局内秘密情報の漏洩や、基地局の複製などが挙げられる。このような状況では、次の要求項目が考えられる。

【０００９】（３）基地局の分解あるいは基地局の複製という状況が生じても、無線端末の正当性確認に利用する秘密情報の漏洩は生じないこと。

【００１０】無線端末の正当性確認に利用する秘密情報を取得した利用者は、本来の利用者に“なりすまし”て通信サービスを享受することができる。この“なりすまし”は、課金処理の根底を脅かすものであり、（３）を満たすことは必須条件となる。　このような無線通信システムのセキュリティ機能を実現する場合、暗号技術を利用することが一般的である。以上の要求項目のうち、（２）と（３）は公開鍵暗号技術の利用により解決できる。

【００１１】具体的には、例えばFiat-Shamir 法で無線端末の正当性を確認できる。Fiat-Shamir 法の詳細は、Fiat, A. and Shmir, A. “How to Prove Yourself:PracticalSolutions to Identification and Signature Problems”, Proc. of CRYPTO'86, Lecture Notes on Computer Science 263, Springer-Verlag, pp. 186-194 に詳しい。

【００１２】しかしながら、Fiat-Shamir 法を無線端末の認証に用いた場合、発呼（あるいは着呼）時の認証処理においては、正当な端末が確かに基地局にアクセスしたことが保証されるが、その認証処理終了後に不正端末が回線に割り込んで不正にアクセスする可能性が残る。

【００１３】また、認証処理終了後、暗号鍵の共有を行い、以降の通信は共有された暗号鍵を用いて、メッセージ認証を行う方法が考えられるが、暗号鍵の共有手続きのために新たな通信が必要となる。暗号鍵の共有のために通信される情報も誤りが許されないため、通話開始ま

でに時間を要する原因となる可能性がある。

【００１４】この問題点に対し、認証処理と暗号鍵共有処理を融合した構成が次の文献に提案されている：T. Okamoto and K. Ohta, "How to Utilize the Randomness of Zero-Knowledge Proofs", Proc. of CRYPTO'90。認証処理で利用される乱数情報を鍵共有情報で構成していることがポイントである。提案されている方式の中で通信量が少ないものを次に示す。

【００１５】文献の方式は、ユーザ１とユーザ２が相互に認証を行い、さらに暗号鍵の共有を行うものである。認証部分に拡張Fiat-Shamir 法による相手確認を用い、鍵共有部分にＤＨ方式を用いている。

【００１６】拡張Fiat-Shamir 法の詳細は、K. Ohta and T. Okamoto , " A Modification ofthe Fiat-Shamir Scheme" Proc. of CRYPTO'88　もしくは、L. C. Guillou and J. J. Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors Both Transmission and Memory ", Proc. of EUROCRYPT'88. に詳しい。

【００１７】また、ＤＨ鍵共有法の詳細は、W. Diffie and M. Hellman, "New Directions in Cryptography", IEEE Trans. IT-22, No. 6, pp. 644-654. に詳しい。

【００１８】サービス提供者は素数ｐ，ｑを生成し、Ｎ＝ｐ・ｑを公開の法の値とする。また、（ｐ－１）および（ｑ－１）と互いに素である整数ｅと公開の底の値ｇを定める。さらに、各ユーザに対し、次式を満たす秘密情報を求め、発行する。

【００１９】

$S_i^e = 1/I_i \bmod N$　　（ｉ＝１、２、…）

但し、Ｉｉはユーザｉの識別番号

処理手順は次の通りである。

【００２０】（１）ユーザ１とユーザ２は互いに識別番号Ｉ１、Ｉ２を交換する。

【００２１】（２）ユーザ１は乱数ｒ１（１＜ｒ１＜Ｎ）を生成し、次式によりＸ１を求め、これをユーザ２に送信する。

【００２２】$X1 = g^{e \cdot r1} \bmod N$

（３）ユーザ２は乱数ｒ２（１＜ｒ２＜Ｎ）を生成し、次式によりＸ２を求める。　　$X2 = g^{e \cdot r2} \bmod N$

さらに、乱数Ｅ１（１＜Ｅ１＜ｅ）を生成し、Ｅ１とＸ２をユーザ１に送信する。

【００２３】（４）ユーザ１は次式により、認証情報Ｙ１を計算する。

【００２４】$Y1 = S1^{E1} \cdot g^{r1} \bmod N$

さらに、乱数Ｅ２（１＜Ｅ２＜ｅ）を生成し、Ｅ２とＹ１をユーザ２に送る。

【００２５】（５）ユーザ２は次式の検査を行う。

【００２６】$X1 = ?Y1^e \cdot I1^{E1} \bmod N$

検査式が成立する場合には、ユーザ１を正当であると判断する。

【００２７】さらに、鍵Ｋを次式により計算する。

【００２８】$K = X1^{r2} \bmod N = g^{e \cdot r1 \cdot r2} \bmod N$

また、認証情報Ｙ２を次式により計算し、ユーザ１に送信する。

【００２９】$Y2 = S2^{E2} \cdot g^{r2} \bmod N$

（６）ユーザ１は次式の検査を行う。

【００３０】$X2 = ?Y2^e \cdot I2^{E2} \bmod N$

検査式が成立する場合には、ユーザ２を正当であると判断する。さらに、鍵Ｋを次式により計算する。

【００３１】$K = X2^{r1} \bmod N = g^{e \cdot r1 \cdot r2} \bmod N$

上記手順によれば、認証処理を行い、その正当性が確認された場合にのみ鍵共有を行うことができる。鍵共有のために新たに通信を必要とすることはない。しかしながら、この方式は、不特定多数の通信者間の鍵生成を、平等に行うために設計されたものであり、相互の認証を行っている。実際の無線端末と基地局の間では、例えば無線端末の認証は必要とされるが基地局の認証は必要としない場面が多い。また、上記手順では（Ｘ１，Ｅ１，Ｙ１，Ｘ２，Ｅ２，Ｙ２）の通信が必要であり、仮に法Ｎのサイズを512 ビットとし、ｅのサイズを64ビットとすると全通信量は2176ビットとなり、通信量がやや多い。なお、この通信量には、識別番号Ｉ１、Ｉ２の通信は含んでいない。識別番号の通信は、認証処理以前に送信されるものと考えられるからである。

【００３２】

【発明が解決しようとする課題】以上述べてきたように、従来技術による端末の正当性確認を無線通信システムに適用した場合、正当な無線端末が認証された後で、不正端末がその回線に割り込んでアクセスする可能性があった。これを防止する方法として、無線端末の認証と暗号鍵の共有を同時に実現する方式も存在するが、対等な２者間での相互認証・鍵共有を前提としているため、通信量が多いことが欠点であった。

【００３３】本発明の目的は、認証部分では無線端末の認証のみを行い、これと基地局－無線端末間の暗号鍵の共有を同時に実現する方式を提供するとともに、基地局－無線端末の相互認証と暗号鍵の共有を同時に実現する方式であって、従来よりも通信量の少ない方式を提供することにある。

【００３４】

【課題を解決するための手段】前述した目的を達成するために、本発明は複数の無線端末と該無線端末からの通信情報を伝送・交換するネットワーク側装置としての複数の基地局および制御局から構成され、各無線端末は装置固有の第１の秘密情報とシステムの公開情報を有し、前記各基地局は、基地局の第２の秘密情報を有する無線通信システムであって、前記基地局が第１の乱数を生成して前記無線端末に送信する工程と、前記無線端末が第２の乱数を生成し、基地局の公開情報を用いて変換する

ことにより鍵配送情報を生成し、前記第１の乱数と前記鍵配送情報と前記第１の秘密情報から認証情報を生成して前記基地局に送信する工程と、前記基地局が、前記第１の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認する工程と、前記基地局が前記第１の乱数と前記鍵配送情報と前記認証情報が、所定の関係を満たすことを確認すると、前記無線端末が前記第２の乱数と前記基地局の公開情報から暗号鍵を求める工程と、前記基地局が、鍵配送情報と基地局の秘密情報から暗号鍵を求める工程と、を具備し、前記基地局が前記無線端末の正当性を確認することを特徴とする無線通信システムの通信方法である。

【００３５】

【作用】本発明は、基地局による無線端末の認証と鍵共有を融合した方式である。各無線通信端末には、自装置固有の秘密情報と基地局の公開情報が発行される。一方、基地局には、基地局の秘密情報が発行される。認証は次の手順で行う。まず、基地局が第１の乱数を生成し、無線端末に送信する。無線端末は、第２の乱数を生成し、これを基地局の公開情報で暗号化して鍵配送情報を生成する。さらに、無線端末は第１の乱数と鍵配送情報に対し、自装置の秘密情報を作用させ認証情報を作成し、鍵配送情報と認証情報を基地局に送信する。基地局は、第１の乱数と鍵配送情報と認証情報が所定の関係式を満たすことを確認することによって無線端末の認証を行う。認証後に、基地局は認証時の鍵配送情報と基地局の秘密情報から暗号鍵を得る。一方、無線端末は、第１の乱数と基地局の公開情報から暗号鍵を得る。

【００３６】さらに、基地局による無線端末の認証と鍵共有を融合することもできる。この場合、無線端末と基地局には、それぞれ、通信相手の識別番号により共有情報を出力する鍵共有関数を発行しておく。この鍵共有関数はそれぞれの装置ごとに異なる。また、各無線端末には自装置固有の秘密情報を発行しておく。基地局による無線端末の認証は、次の手順で行う。基地局と無線端末が共に乱数を生成する。無線端末は、この２種類の乱数に秘密情報を作用させて認証情報を生成する。基地局は、前記２種類の乱数と認証情報が所定の関係式を満たすことを確認することで行う。これが確認された場合に、認証時に交換した情報と相手識別番号により無線端末と基地局が暗号鍵を共有する。認証時に交換した情報を鍵共有関数の入力の一つとすることにより、共有される鍵の値が毎回変わり、認証処理と鍵共有処理が連結される。

【００３７】また、無線端末と基地局の相互認証と鍵共有を融合することもできる。この場合、無線通信端末および基地局には、それぞれ自装置固有の秘密情報を発行しておく。さらに各々の装置に共通の乱数生成関数を備える。無線端末と基地局が相互に正当性を確認する手順を次の考え方のもとに行う。基地局と無線端末は、相互の鍵共有に必要な鍵共有情報を作成し、これを相互に通信する。相互認証時に必要な乱数は、前記鍵共有情報と乱数生成関数から生成する。相互の装置の正当性が確認された場合に前記鍵共有情報から共通の暗号鍵を生成する。相互認証に必要な乱数を鍵共有情報と装置内の関数から構成するために、通信により交換する乱数の数を減らすことができ、通信量の削減になる。

【００３８】

【実施例】以下、図面を参照して本発明の実施例を説明する。

【００３９】まず、無線通信システムの構成を図２に示す。無線端末には、それぞれ固有の識別番号（PSi ）が与えられ、さらに固有の秘密情報（S_{PSi}）が発行される。ネットワーク側は、制御局ＣＣと複数の基地局CS_1、…CS_nからなる。全基地局には共通の基地局秘密情報が発行される。制御局ＣＣには、各々の無線端末に対する課金情報などを蓄積したデータベースが存在する。基地局CS_iにはデータベースは存在しない。基地局CS_iと無線端末PS_i間の通信は、無線が利用されるが、基地局CS_iと制御局ＣＣの間の通信は、有線もしくは無線である。無線端末PS_iの正当性の確認および無線回線で用いる暗号方式用の暗号鍵の共有は、無線端末PS_iと基地局CS_iの間で行われ、中央の制御局ＣＣにアクセスする必要はない。このような認証方式が実行されるのは、無線端末PS_iからの発信時、別の無線端末PS_kへの着信時などである。

【００４０】図１に本発明による無線端末の認証・鍵共有方式を示す。

【００４１】（１）無線端末から基地局へ、無線端末の識別番号PSi が送信される。

【００４２】…（ステップ101 ）

（２）基地局は、第１の乱数Ｒ１を生成し、無線端末に送信する。

【００４３】…（ステップ102 ）

（３）無線端末は、第２の乱数Ｒ２を生成し、Ｒ１とＲ２と秘密情報S_{PSi}とを認証情報作成手段１０３により合成し、認証情報σ_{PS}を得る。

【００４４】…（ステップ103 ）

認証情報σ_{PS}と第２の乱数Ｒ２を基地局に送信する。…（ステップ104 ）

（４）基地局は、第１の乱数Ｒ１と第２の乱数Ｒ２と無線端末の識別番号PSi と認証情報σ_{PS}を認証情報検査手段１０５に通し、結果がＯＫの場合には、無線端末をPS i であるものと認証する。結果がＮＧの場合には、不正端末であるとして、処理を終了する。

…（ステップ105 ）

（５）上記認証処理に成功した場合、無線端末と基地局は、共通の暗号鍵を鍵共有手段１０６ａ、１０６ｂにより生成する。このとき、新たに情報の交換を行わず、上記認証処理で交換した情報および自装置内に予め格納さ

れていた情報のみを利用する。
…（ステップ106 ）
上記手順のうち、（２）から（４）の無線端末の正当性確認部分は、ＩＤ情報に基づく相手確認法あるいは、ＩＤ情報に基づくディジタル署名法を利用したチャレンジ・レスポンス方式で構成する。このような方法で構成することの利点として次のことが挙げられる。
①基地局側に必要な情報は、無線端末の識別番号と基地局の公開情報、基地局の秘密情報のみであり、基地局が分解されても無線端末の秘密情報は存在しない。さらに、通信情報から無線端末の秘密情報は漏洩しない。従って、無線回線上の情報の盗聴やニセ基地局相手に認証処理を行った場合にも安全性が確保できる。無線端末の作用させる乱数が秘密情報の漏洩を防ぐ。
【００４５】②互いの装置が毎回乱数を作用させるので、ある時点で正当な無線端末から送信された認証情報を通信回線上で盗み、それを再送したとしても、認証処理を通過できない。
【００４６】③①で指摘したように、認証時に相手装置の識別番号の送信が必要となるが、この情報は、認証処理以前に送信される可能性があるため、通信量が削減できる。ＩＤ情報に基づく方式でないディジタル署名方式（例えばＲＳＡ暗号など）を利用する場合には、無線端末固有の公開情報とその正当性証明情報（KohnfelderによるPublic Key Certificateなど）の送信が必要であり、その分通信量が増加する。
【００４７】ＩＤ情報に基づく相手確認法およびディジタル署名法の具体例には、次の方式がある。
【００４８】・Fiat-Shamir 法：A Fiat and A. Shamir, “How to Prove Yourself ”, Proc. ofCRYPTO’86 .
・拡張Fiat-Shamir 法：K. Ohta and T. Okamoto , “ A Modification of the Fiat-Shamir Scheme ”, Proc. of CRYPTO’88.
もしくは、L. C. Guillou and J. J. Quisquater, “A Practical Zero-Knowledge Protocol Fitted to Security Microprocessors Both Transmission and Memory”, Proc. of EUROCRYPT’88.
・拡張Fiat-Shamir 法２：太田和夫、“ＲＳＡ暗号を利用したＩＤに基づく認証方式とその応用”，第１１回情報理論とその応用シンポジウム予稿集，pp. 567-572.
・Beth法：T. Beth, “Efficient Zero-Knowledge Identification Scheme for Smart Cards”, Proc. of EUROCRYPT’88.
上記の中で通信量が少なく、無線端末システムの認証に適する方式として、拡張Fiat-Shamir 法１と２が挙げられる。以降の実施例では、拡張Fiat-Shamir 法１による相手確認法およびディジタル署名法を認証部分に利用している。

$$R2 = g^{r} \bmod N$$
$$X = R2^{e} \bmod N$$
$$E = h(X, R1)$$
$$\sigma_{PS} = S_{PSi}^{E} \cdot R2 \bmod N$$

認証情報σ_{PS}およびＥを基地局に送信する。 …（ステップ303 ）
（ステップ304 ）

【００４９】図１の手順（５）の鍵共有処理では、余分な通信を必要としないため、全体の通信量は、（２）から（４）の認証部分の通信量に等しい。認証部分の通信量は、通常の相手確認の通信量と同じであるので、全体の通信量が少ない。
【００５０】図３には、認証手順を拡張Fiat-Shamir 法による署名により実現し、鍵共有手順をＤＨ鍵共有法により実現した実施例を示す。
【００５１】まず、サービス提供者は次の準備を行う必要がある。まず、２つの素数ｐ，ｑを定め、その積をＮとする。また、（ｐ－１）と（ｑ－１）の最小公倍数をＬとし、Ｌと互いに素である整数ｅを定める。さらに、GF(p)，GF(q) で共に原始根となる整数ｇを定める。また、基地局の秘密情報ｔ（１＜ｔ＜Ｌ）を定め、基地局の公開鍵Ｇを

$$G = g^{t} \bmod N$$

で求める。無線端末PSi に対しては、次式を満たす秘密情報S_{PSi}を求め、秘密に発行する。
【００５２】$S_{PSi}^{e} = PSi \bmod N$
但し、PSi は無線端末PSi の識別番号
さらに、一方向性の圧縮関数ｈ（）を定める。例えば、ブロック暗号ＤＥＳ(Data Encryption Standard)のＣＢＣモードで構成した関数をｈ（）とする。
【００５３】以上で生成した情報を次のように管理する。
①基地局の公開情報（全無線端末と全基地局に発行する）：Ｎ，ｇ，Ｇ，ｅ，ｈ（）
②基地局の秘密情報（全基地局に発行する）：ｔ
③無線端末の秘密情報（無線端末PSi に発行する）：S_{PSi}
④サービス提供者の秘密情報：ｐ，ｑ，Ｌ
処理の手順は次のようになる。
【００５４】（１）無線端末は、基地局に自装置の識別番号PSi を送信する。
【００５５】…（ステップ301 ）
（２）基地局は、第１の乱数Ｒ１（１＜Ｒ１＜Ｎ）を生成し、Ｒ１を無線端末に送信する。
…（ステップ302 ）
（３）無線端末は、乱数ｒ（１＜ｒ＜Ｎ）を生成し、次式の計算を実行する。
【００５６】

（４）基地局は、次式の計算を行う。

【００５７】$X' = \sigma_{PS}^{e} / PSi^{g} \bmod N$

無線端末から送信されたＥと次式の右辺が一致するかど＊うか確認する。

$E = ?\ h\ (X', R1)$　…（ステップ305）

（５）基地局は、（４）において無線端末の正当性を確認した場合、次の計算により暗号鍵Ｋを求める。　※

【００５８】

$K = X'^{t} \bmod N = g^{e \cdot r \cdot t} \bmod N$　…（ステップ306）

※【００５９】

一方、無線端末は、次の計算により暗号鍵Ｋを求める。

【００６０】

$K = G^{r} \bmod N = g^{e \cdot r \cdot t} \bmod N$　…（ステップ307）

上記方式の鍵共有方式では、離散対数問題（$G = (g^{e})^{t} \bmod N$の値からｔの値を求めること。もしくは、$X = (g^{e})^{r} \bmod N$の値からｒの値を求めること）が困難である限り、第三者は暗号鍵の値を求められない。

【００６１】上記方式の通信量は、法Ｎのサイズを512ビット、一方向性関数ｈの出力を64ビット、乱数Ｒ１を64ビットと仮定すると、640 ビットである。

【００６２】図４には、認証手順を拡張Fiat-Shamir 法の署名方式で実現し、さらに、無線端末と基地局の安全な装置構成を前提とした鍵共有方式による実施例を示す。

【００６３】（１）無線端末は、基地局に自装置の識別番号PSi を送信し、基地局は、無線端末に自装置の識別番号CSj を送信する。　…（ステップ401）

（２）基地局は、乱数Ｒ１（１＜Ｒ１＜Ｎ）を生成し、★

★無線端末に送信する。

【００６４】…（ステップ402）

（３）無線端末は、乱数Ｒ２（１＜Ｒ２＜Ｎ）を生成し、次式の計算を実行する。　$X = R2^{e} \bmod N$

$E = h\ (X, R1)$

$\sigma_{PS} = S_{PSi}^{g} \cdot R2 \bmod N$　…（ステップ403）

認証情報σ_{PS}およびＥを基地局に送信する。　…（ステップ404）

（４）基地局は、次式の計算を行う。

【００６５】$X' = \sigma_{PS}^{e} / PSi^{g} \bmod N$

無線端末から送信されたＥと次式の右辺が一致するかどうか確認する。

$E = ?\ h\ (X', R1)$

【００６６】

…（ステップ405）

（５）基地局は、（４）において無線端末の正当性を確認した場合、自装置内の関数f_{CSj}に無線端末の識別番号PSi と乱数Ｒ１とＸ´を入力して共有鍵Ｋを求める。　…（ステップ406）

一方、無線端末は、自装置内の関数f_{PSi}に基地局の識別番号CSj と乱数Ｒ１とＸを入力して共有鍵Ｋを求める。　…（ステップ407）

なお、乱数Ｒ１とＸ（あるいはＸ´）を利用する代わりにＥを入力するようにしてもよい。

【００６７】上記方式の通信量は、図３に示す実施例と同様640 ビットである。

【００６８】図４に示す実施例において（４）の鍵共有部で利用する関数f_{psi}(501) とf_{CSj}(502) の一例を図５に示す。図５における関数ｆ(503) は秘密であり、多入力の関数である。無線端末の識別番号PSi(504)と基地局の識別番号CSj(505)、さらに認証処理で使用された乱数情報(506) を入力する構成である。これらの乱数情報の入力により、認証処理ごとに異なる鍵Ｋ(507) が共有される。無線端末側の関数f_{PSi}は、自装置の識別番号PSi の関数ｆへの入力が変更できないように装置構成されている。すなわち、PSi の入力(504) の部分に、他の無線端末の識別番号PSj を入力することができないように構成されている。基地局側の関数f_{CSj}も同様に、自装置の識別番号CSj が変更できないように装置構成されている。これらの構成することにより、不正端末が無線端末PSi と基地局CSj の間の鍵を共有することが不可能になる。

【００６９】このような装置構成により暗号鍵の共有部分を実現した場合、その装置構成を破られると鍵共有の安全性は保証されない。しかし、このことは、認証部分の安全性には、影響しない。

【００７０】次に、基地局と無線端末が相互に認証を行いながら、鍵共有を行う方式の実施例を説明する。この場合には、基地局にも、それぞれ固有の秘密情報S_{CSj}が発行される。

【００７１】図６に無線端末と基地局の相互認証・鍵共有方式の一基本構成を示す。

【００７２】（１）無線端末から基地局へ、無線端末の識別番号PSi が送信される。また、基地局から無線端末へ、基地局の識別番号CSj が送信される。

【００７３】…（ステップ601）

（２）基地局は、第１の乱数Ｒ１を生成し、無線端末に送信する。

【００７４】…（ステップ602）

（３）無線端末は、第２の乱数Ｒ２を生成し、Ｒ１とＲ２と秘密情報S_{PSi}とを認証情報作成手段により合成し、認証情報σ_{PS}を得る。

【００７５】…（ステップ603）

この認証情報σ_{PS}と第２の乱数Ｒ２を基地局に送信す

る。

【００７６】…（ステップ604 ）

（４）基地局は、Ｒ１とＲ２と無線端末の識別番号PSiと認証情報σ_{PS}を認証情報検査手段に通し、結果がＯＫの場合には、無線端末をPSi であるものと認証する。結果がＮＧの場合には、不正端末であるとして、処理を終了する。

…（ステップ605 ）

さらに、Ｒ１とＲ２と秘密情報S_{CSj}とを認証情報作成手段により合成し認証情報σ_{CS}を得る。

…（ステップ606 ）

この認証情報σ_{CS}を無線端末に送信する。…（ステップ607 ）

（５）無線端末は、Ｒ１とＲ２と基地局の識別番号CSjと認証情報σ_{CS}を認証情報検査手段に通し、結果がＯＫの場合には、基地局をCSj であるものと認証する。結果がＮＧの場合には、不正基地局であるとして、処理を終了する。

…（ステップ608 ）

（６）上記認証処理に成功した場合、無線端末と基地局は、共通の暗号鍵を鍵共有手段により生成する。このとき、新たに情報の交換を行わず、上記認証処理で交換した情報および自装置内に予め格納されていた情報のみを利用する。

…（ステップ609 ）

この手順は、図１の基本構成を双方向にしたものである。図１の基本構成では、無線端末のみの認証を行う目的で、乱数を基地局と無線端末のそれぞれが生成し、相手装置に送信していた。上記手順では、相互の認証を行う目的に対して、無線端末の認証のみを行う場合と同数の乱数を利用することにとどめている。このときに不足する乱数を補うために、一方向性のランダム関数を全装置に備えておき、相手装置からの送信情報をランダム関数に作用させた結果を利用する。通信により交換する乱数が少なくなる分、通信量が減少する。

＊

$$R1 = g^{r1} \bmod N$$

$$X1 = R1^{\cdot} \bmod N$$

Ｘ１を無線端末に送信する。…（ステップ703 ）

（３）無線端末は、乱数ｒ２（１＜ｒ２＜Ｎ）を生成　※

$$R2 = g^{r2} \bmod N$$

$$X2 = R2^{\cdot} \bmod N$$

Ｘ２を基地局に送信する。…（ステップ705 ）

（４）基地局は、関数ｈにＸ２を入力することにより、Ｅ１を得る。　★

$$Y_{CS} = S_{CSj}{}^{E1} \cdot R1 \bmod N$$

認証情報Y_{CS}を無線端末に送信する。…（ステップ707 ）

（５）無線端末は、基地局CSj の正当性を次式の計算・

＊【００７７】図７には、拡張Fiat-Shamir 法による相手確認による相互認証とＤＨ法による鍵共有法を融合した実施例を示す。

【００７８】まず、サービス提供者は次の準備を行う必要がある。まず、２つの素数ｐ，ｑを定め、その積をＮとする。また、（ｐ－１）と（ｑ－１）の最小公倍数をＬとし、Ｌと互いに素である整数ｅを定める。さらに、GF(p) , GF(q) で共に原始根となる整数ｇを定める。無線端末PSi に対しては、次式を満たす秘密情報S_{PSi}を求め、秘密に発行する。

【００７９】$S_{psi}{}^{\cdot} = PSi \bmod N$

但し、PSi は無線端末PSi の識別番号

また、基地局CSj に対しても同様に次式を満たす秘密情報S_{CSj}を求め、秘密に発行する。

【００８０】$S_{CSj}{}^{\cdot} = CSj \bmod N$

但し、CSj は基地局CSj の識別番号

さらに、一方向性の圧縮関数ｈ（）を定める。例えば、ブロック暗号ＤＥＳ(Data Encryption Standard)のＣＢＣモードで構成した関数をｈ（）とする。

【００８１】以上で生成した情報を次のように管理する。

【００８２】①システムの公開情報（全無線端末と全基地局に発行する）：Ｎ，ｇ，ｅ，ｈ()

②基地局の秘密情報（基地局CSj に発行する）：S_{CSj}

③無線端末の秘密情報（無線端末PSi に発行する）：S_{PSi}

④サービス提供者の秘密情報：ｐ，ｑ，Ｌ

処理手順は次の通り。

【００８３】（１）無線端末から基地局へ識別番号PSi が送信される。一方、基地局から移動端末へ識別番号CSj が送信される。…（ステップ701 ）

（２）基地局は、乱数ｒ１（１＜ｒ１＜Ｎ）を生成し、次式の計算を行う。

【００８４】

…（ステップ702 ）

※し、次式の計算を行う。

【００８５】

…（ステップ704 ）

★【００８６】Ｅ１＝ｈ（Ｘ２）

このＥ１と秘密情報S_{CSj}，Ｒ１とから次式の計算を行う。

【００８７】

…（ステップ706 ）

検査により行う。

【００８８】

Ｅ１＝ｈ（Ｘ２）

Y_{CSe} ＝？ CSj^{E1}・Ｘ１mod Ｎ

この関係式が成立した場合には、基地局を正当であると判断する。

【００８９】…（ステップ708 ）

Ｅ２＝ｈ（Ｙ１）

$Y_{PS}=S_{PSi}^{E2}$・Ｒ２mod Ｎ

認証情報Y_{PS}を基地局に送信する。…（ステップ710 ）

（６）基地局は、無線端末PSi の正当性を次式の計算・検査により行う。

【００９２】

Ｅ２＝ｈ（Ｙ１）

Y_{CS}^{e}＝？ PSi^{E2}・Ｘ２mod Ｎ

上記方式の、ステップ702, 706, 708 は、基地局の正当性に対する拡張Fiat-Shamir の相手確認法とみなすことができる。この中でＸ２を相手確認に利用する検証者の乱数情報とみなしている。一方、ステップ704, 709, 712 は、無線端末の正当性に関する拡張Fiat-Shamir の相手確認法とみなすことができる。この中で、Y_{CS}を検証者乱数情報とみなしている。Y_{CS}の値は、ステップ707 の時点まで無線端末には予測ができないので、こうした利用が可能である。なお、上記方式では、基地局が先にその正当性を証明する手順であるが、逆に無線端末が先に正当性を証明する手順にしてもよい。

【００９５】上記方式は、従来技術の項に記述した岡本ー太田による鍵共有法とほぼ同様の手順であるが、上記方式の特徴は、検証者の乱数Ｅ１、Ｅ２をそれぞれＸ２、Ｙ１（前記手順ではY_{CS}）から生成するようにしている点である。このことにより、Ｅ１、Ｅ２の伝送が不

Ｒ１＝g^{r1}mod Ｎ

Ｘ１＝$R1^{e}$mod Ｎ

Ｘ１を無線端末に送信する。…（ステップ803 ）

（３）無線端末は、乱数ｒ２（１＜ｒ２＜Ｎ）を生成

Ｒ２＝g^{r2}mod Ｎ

Ｘ２＝$R2^{e}$mod Ｎ

Ｅ２＝ｈ（Ｘ１，Ｘ２）

$Y_{PS}=S_{PSi}^{E2}$・Ｒ２mod Ｎ

Y_{PS}とＥ２を基地局に送信する。…（ステップ805 ）

（４）基地局は、次の手順により無線端末の認証を行う。

【０１０２】

Ｘ２´＝Y_{PS}^{e}／ PSi^{E2}mod Ｎ

Ｅ２＝？ｈ（Ｘ１，Ｘ２´）

Ｅ１＝ｈ（Y_{PS}）

＊検査が成功した場合、次式により認証情報Y_{PS}を計算する。

【００９０】

…（ステップ709 ）

※さらに、暗号鍵Ｋを次式の計算により求める。

【００９１】

…（ステップ711 ）

★この関係式が成立した場合には、無線端末を正当であると判断する。

【００９３】…（ステップ712 ）

さらに、暗号鍵Ｋを次式の計算により求める。

【００９４】

…（ステップ713 ）

☆要となっている。Ｅ１、Ｅ２も伝送誤りの許されない情報であることから、無線通信システムの認証・鍵共有では、前記図７の手順の方が通信量の少ない分だけ有効となる。

【００９６】上記方式の通信量は、法Ｎのサイズを512ビットと仮定すると、2048ビットである。

【００９７】図８には、拡張Fiat-Shamir 法によるディジタル署名と相手確認をそれぞれの認証方式に利用し、鍵共有方式にＤＨ方式を利用した実施例を示す。

【００９８】処理手順は次の通り。

【００９９】（１）無線端末から基地局へ識別番号PSiが送信される。一方、基地局から移動端末へ識別番号CSｊが送信される。…（ステップ801 ）

（２）基地局は、乱数ｒ１（１＜ｒ１＜Ｎ）を生成し、次式の計算を行う。

【０１００】

…（ステップ802 ）

◆し、次式の計算により認証情報Y_{PS}を求める。

【０１０１】

…（ステップ804 ）

この関係式が成立した場合には、無線端末を正当であると判断する。

【０１０３】…（ステップ806 ）

検査に通った場合、次式により認証情報Y_{CS}を計算する。

【０１０４】

15

$$Y_{CS}=S_{CSj}^{E1}\cdot R1 \bmod N$$

認証情報Y_{CS}を無線端末に送信する。…（ステップ808 ）

（５）無線端末は、基地局CSj の正当性を次式の計算・検査により行う。

【０１０６】

$E1=h(Y_{PS})$

$$Y_{CS}{}'=?\ CSj^{E1}\cdot X1 \bmod N \quad ※$$

$$K=X1^{r2} \bmod N=g^{r1\cdot r2} \bmod N$$

図８の手順において、ステップ804 のY_{PS}は、Ｘ１に対する拡張Fiat-Shamir署名となっている。一方、ステップ802 のＸ１とステップ807 のY_{CS}は、拡張Fiat-Shamir の相手確認法となっているとみなすことができる。このとき、Y_{PS}の値は基地局にとって予測できないものであり、これを相手確認法における乱数として利用している。

【０１０９】上記方式の通信量は、法Ｎのサイズを512ビット、一方向性関数ｈの出力値を64ビットと仮定すると、1600ビットである。

【０１１０】次に、無線端末ＰＳが、制御局ＣＣによって自分の公開鍵と無線端末のＩＤに関してなされたディジタル署名をされたものを、基地局ＣＳに送信し、基地局ＣＳがこれを無線端末ＰＳの認証に用いることで、不正使用を防止する方式について述べる。

【０１１１】図９において、制御局ＣＣで、無線端末ＰＳｉの公開鍵Ｋｅｉ及びＰＳｉのＩＤ番号ＩＤｉに対して、制御局ＣＣの秘密鍵Ｋｄｃｃによって署名を行う。署名の結果Ｓ１をあらかじめ無先端末ＰＳｉに持たせる。

【０１１２】無線端末ＰＳｉは、認証開始時に、自らのＩＤ番号ＩＤｉと上記の署名の結果Ｓ１を、基地局ＣＳｉに送信する。あらかじめ制御局ＣＣの公開鍵Ｋｅｃｃを記憶している基地局ＣＳｉは、署名の結果、Ｓ１を公開鍵Ｋｅｃｃで検査を行い、出力された結果のうち、ＩＤ番号にあたる部分が無線端末ＰＳｉのＩＤ番号ＩＤｉと同一か否かを比較する。この比較により、先の検査の出力結果のうち残りの公開鍵の部分を無線端末ＰＳｉの公開鍵Ｋｅｉと認識する。

【０１１３】次に、基地局ＣＳｉはあるメッセージＭを無線端末ＰＳｉに送出する。受信した無線端末ＰＳｉは、メッセージＭに対してハッシュ関数を用いて圧縮処理した結果に対して、無線端末ＰＳｉの秘密鍵Ｋｄｉを用いて署名を行う。署名結果Ｓ２を基地局ＣＳｉへ送出する。ＣＳｉは、署名結果Ｓ２を先の検査で出力された無線端末ＰＳｉの公開鍵Ｋｅｉを用いて検査する。この検査結果を、メッセージＭに対して無線端末ＰＳｉと同一のハッシュ関数で圧縮処理した結果と比較し、認証に用いることで、不正使用を防止することができる。

【０１１４】ここで、単純化のためハッシュ関数による

16

…（ステップ807 ）

＊さらに、暗号鍵Ｋを次式の計算により求める。

【０１０５】

$$K=X2^{r1} \bmod N=g^{r1\cdot r2} \bmod N$$

…（ステップ809 ）

※この関係式が成立した場合には、基地局を正当であると判断する。

【０１０７】…（ステップ810 ）

さらに、暗号鍵Ｋを次式の計算により求める。

【０１０８】

$$K=X1^{r2} \bmod N=g^{r1\cdot r2} \bmod N$$

…（ステップ811 ）

双方での圧縮処理を省略することも考えられる。また、無線端末ＰＳｉに関する認証を考えたが、契約している無線端末の使用者に関する認証に関しても、パーソナルＩＤの入ったＩＣカードを無線端末に挿入などの作用をすることにより、同様の効果を得ることができる。以下の実施例でも同じことが言える。

【０１１５】本実施例に拠れば、制御局ＣＣ側に公開鍵のＤＢを持たせたり、制御局ＣＣにアクセスすることなく、公開鍵による認証を行うことができる。したがって、マイクロセル方式を用いた場合に飛躍的に増大する基地局ＣＳと制御局ＣＣや交換機などとの間でやりとりされる情報量を極力減らすことができる。

【０１１６】一方、マイクロセル方式では基地局ＣＳは小形になり、設置場所も従来のビルの屋上などから、建物の壁の低い位置など一般の通行人の目に触れやすい場所になり、盗難の恐れが増える。また、一部は、電池駆動になったり、制御局とのリンクを無線で張ったりすることが考えられ、この場合は、盗難の恐れがさらに増大し、盗難された時の悪意を持った改造がより簡単になる恐れがある。しかし、本実施例に拠れば、基地局ＣＳが盗難されたとしても、慣用暗号を用いた認証のために用いる秘密鍵をＲＯＭなどから読み出された場合に比べ、偽の認証データの捏造や悪用の可能性は極めて低くなる。

【０１１７】また、慣用暗号を用いた認証を採用した場合、悪意をもって偽の基地局ＣＳを構成し、通話開始前の認証用情報のやり取りから、端末に記憶されている秘密鍵などの秘密情報を吸い上げてしまう行為を許してしまう可能性がある。しかし、公開鍵暗号を用いた本実施例に拠れば、このような行為を許す可能性はなくなる。

さらに、複数のサービス提供者の間で、相互ハンドオフサービスを行う場合、ハンドオフの際にあらためて認証を必要とする可能性がある。このときも、制御局側にアクセスすることなく認証が行えるため、ハンドオフにかかる時間の短縮化にも寄与する。

【０１１８】加えて、無線端末ＰＳによる基地局ＣＳの認証にも同様の手続きを適用することも考えられる。

【０１１９】図１０に示す実施例は、片方向のみの送受信を用いることで、認証に要する時間の低減を図ったものである。

【０１２０】前半の署名の結果Ｓ１とＩＤ番号ＩＤｉの伝送にかかわる処理は、図９に示す実施例と同様である。

【０１２１】次に、無線端末ＰＳｉはあるメッセージＭに対してハッシュ関数を用いて圧縮処理した結果に対して、無線端末ＰＳｉの秘密鍵Ｋｄｉを用いて署名を行う。署名結果Ｓ２とメッセージＭを基地局ＣＳｉへ送出する。基地局ＣＳｉは、署名結果Ｓ２を先の検査で出力された無線端末ＰＳｉの公開鍵Ｋｅｉを用いて検査する。この検査結果、メッセージＭに対して無線端末ＰＳｉと同一のハッシュ関数で圧縮処理した結果と比較し、認証に用いることで、不正使用を防止することができる。

【０１２２】ここで、単純化のためハッシュ関数による双方での圧縮処理を省略することも考えられる。

【０１２３】本実施例では、署名結果Ｓ２とメッセージＭとの送出を連続して行い、署名結果Ｓ２の処理とメッセージＭの送出を時間的に並列に行うことができるため、認証に要する時間が低減できる。

【０１２４】ただし本実施例では、片方向のみの伝送が行われるため、この一連の伝送の履歴を盗聴された場合に、同一手順を踏むことによって認証手続きが破られる恐れがある。しかし、メッセージＭに現在の年月日および時刻を用いることなどによって、ある程度の安全性を与えることができる。

【０１２５】図１１に示す実施例では、認証に要する情報（以下、これを認証用情報と称する）を、適当な長さのバーストに分割し、個々のバーストについて自動再送手順を用いるものである。

【０１２６】図１２、図１３に、仮定する２種類のバースト構成を示す。

【０１２７】図１２に示すバーストは、過渡応答用ランプタイムＲ（４ビット）、スタートシンボルＳＳ（２ビット）、プリアンブルＰＲ（６ビット）、同期ワードＵＷ（１６ビット）、情報ビットＩ（１９６ビット）と１６ビットのガードビットからなる。情報ビットＩは、図１２（ｂ）に示すように、チャネル種別ＣＩ（４ビット）、低速付随制御チャネルＳＡ（１６ビット）、トラヒックチャネルＴＣＨ（１６０ビット）、ＣＲＣ（１６ビット）からなる。

【０１２８】図１３に示すバーストは、過渡応答用ランプタイムＲ（４ビット）、スタートシンボルＳＳ（２ビット）、制御信号ＣＡＣ（６２ビット）、同期ワードＵＷ（３２ビット）、制御信号ＣＡＣ（１２４ビット）と１６ビットのガードビットからなる。６２ビットの制御信号ＣＡＣは、図１３（ｂ）に示すユーザ特定制御チャネルＵＳＣＣＨであり、１２４ビットの制御信号ＣＡＣは、チャネル識別ＣＩ（４ビット）、発識別符号（４２ビット）、着識別符号（２８ビット）、ユーザ特定制御チャネルＵＳＣＣＨ（３４ビット）、ＣＲＣ（１６ビット）からなる。　図１２および図１３に示すバーストのうちいずれのフォーマットも１６ビットのＣＲＣの検出ビットを備えており、誤り検出が可能である。

【０１２９】図１２に示すフォーマットでは、１バーストあたり情報ビットＩの１９６ビットがＣＲＣ検査ビットとＣＲＣを掛けられるビットを加えた値である。図１３に示すフォーマットでは、１バーストあたり制御信号ＣＡＣの６２＋１２４＝１８６ビットがＣＲＣ検査ビットとＣＲＣを掛けられるビットを加えた値である。

【０１３０】このうち、図１２に示すフォーマットでは、１バーストあたり低速付随制御チャネルＳＡとトラヒックチャネルＴＣＨの１６＋１６０＝１７６ビットが認証用情報の送受に使用できる。また、図１３に示すフォーマットでは、１バーストあたりユーザ特定制御チャネルＵＳＣＣＨの６２＋３４＝９６ビットが認証用情報の送受に使用できる。

【０１３１】このバースト構成に沿ったＣＲＣで誤りを検出する機能を用いた時に、認証用情報を全て送り終えるまでの時間を見積もる。ここでは、通信における呼損率を１％とし、これと同じ程度の確率の失敗は許容するものとする。

【０１３２】ＣＲＣ１６ｂｉｔを用いたとき、本当は誤りがあるのに見逃す確率は、2^{-16}、おおよそ1.5×10^{-5}でおさえられる。これは上記の１％より十分小さいので、ＣＲＣはほぼ完全に誤りを発見できると仮定する。

【０１３３】このとき、伝送路の平均ビット誤り率をεとすると、ＣＲＣ検査ビットとＣＲＣをかけられるビットの計ｎビットが全て誤りなしで伝送できる確率（スループット）ηは、$\eta=(1-\varepsilon)^n$となる。

【０１３４】ここで、伝送路のビット誤り率の最悪値10^{-2}を当該伝送路がとるとすると、スループットηは、図１２のフォーマットを用いた場合では、０．１３９，図１３のフォーマットでは、０．１５４となる。

【０１３５】一方、認証方式として、ＲＳＡ、エルガマルの両方式を候補とすると、署名をして送り返すビット数は、５１２、１０２４、２０４８の３通りが考えられる。これだけのビット数を前述のフォーマットを用いて分割して送る場合に必要なバーストの数をＫとすると、図１２のフォーマットで５１２ビット送受するにはＫ＝３であり、図１３のフォーマットで２０４８ビット送受するには、Ｋ＝２２である。

【０１３６】また、認証に費やしてよい時間をｔ秒とすると、図１２、図１３のフォーマットとも１バースト送信するのに５ミリ秒を要するから、ｔ秒間に送信できるバーストの数はＮは、$N=t/(5\times10^{-3})=200t$である。

【０１３７】ここで、上記のビット数だけの認証用情報を誤り無く全てを送ることに失敗する確立は、「スループットηのパケット通進路で、Ｎ回パケットを送信したが、Ｋ回未満しか誤り無く送れない確率Ｐ」に等しい。

すなわち、

$$P=(1-\eta)^{N}+{}_{N}C_{1}\times\eta\times(1-\eta)^{N-1}+\cdots\cdots$$
$$\cdots\cdots+{}_{N}C_{K-1}\times\eta^{K-1}\times(1-\eta)^{N-K+1} \qquad (1)$$

このＰを計算すると、図１２のフォーマットで５１２ビット送受する場合、Ｎ＝３０でＰは約６．９%、Ｎ＝６０でＰは約０．７%となる。したがって９９..３%の確率で認証用情報の送信を完了するには約０．３秒かかる。図１３のフォーマットで２０４８ビット送受するには、Ｎ＝２００でＰは約２．９%、Ｎ＝２２５でＰは約０．０５%となり、９９．９５%の確率で認証用情報の送信を完了するには約１．１２５秒かかる。

【０１３８】なお、認証を受ける側が上記のような認証用情報を送り返す前に、認証をする側が認証を受ける側に送るデータの長さは、せいぜい上記の送り返す情報の長さ以下である。

【０１３９】（１）の計算からわかるように、確率Ｐは、送信完了に必要なバーストの数によって大きく左右される。

【０１４０】したがって、認証に関わる往復の伝送に必要な時間は、図１２のフォーマットで５１２ビット送受する場合では、最小０．３秒、最大０．６秒、図１３のフォーマットで２０４８ビット送受する場合では、最小１．１２５秒、最大２．２５秒となる。　また、通常のハードウェアで処理を行うＲＳＡ暗号を用いた認証の場合、認証を受ける側が上記のような認証用情報を生成するのに必要な計算処理の時間は、０．１～２秒程度である。

【０１４１】したがって、認証に伴う情報の送受と処理に要する時間は、合計すると０．４～４．２５秒程度と＊

$$\{1-(1-\eta)^{N}\}^{K}$$

この確率を９９%以上にするために必要な各バーストの送出回数Ｎを（２）式から計算すると、図１２のフォーマットで５１２ビット送受する場合、３９回となる。したがって９９%の確率で認証用情報の送信を完了するには

（０．００５秒×３９）×３＝０．５８５秒

かかる。図１３のフォーマットで２０４８ビット送受するには、４６回となり、９９%の確率で認証用情報の送信を完了するには

（０．００５秒×４６）×２２＝５．０６５秒

かかる。

【０１４９】また既述の通り、認証を受ける側が上記のような認証用情報を送り返す前に、認証をする側が認証を受ける側に送るデータの長さは、せいぜい上記の送り返す情報の長さ以下である。

【０１５０】（２）の計算からわかるように、認証用情報送出に必要な時間は、分割バースト数Ｋに大きく左右される。

【０１５１】したがって、認証に関わる往復の伝送に必要な時間は、図１２のフォーマットで５１２ビット送受＊なる。

【０１４２】本実施例に拠れば、確実な認証用情報の送受が、比較的短い時間で可能となる利点がある。

【０１４３】なお、ここでは誤り検出符号のみを適用したが、誤り訂正符号を併用し、伝送路のスループットを向上することも考えられる。

【０１４４】図１４に示す実施例では、認証用情報を、適当な長さのバーストに分割し、複数回送信するものである。

【０１４５】ここでは、既述の第２の実施例のバースト構成例を利用して説明する。

【０１４６】既述の通り、認証方式として、ＲＳＡ、エルガマルの両方式を候補とすると、署名をして送り返すビット数は、５１２、１０２４、２０４８の３通りが考えられる。これだけのビット数を前述のフォーマットを用いて分割して送る場合に必要なバーストの数をＫとすると、図１２のフォーマットで５１２ビット送受するにはＫ＝３であり、図１３のフォーマットで２０４８ビット送受するには、Ｋ＝２２である。

【０１４７】ここで、必要な各バーストの送出回数をＮとする。スループットηのパケット通進路で、Ｎ回パケットを送信して少なくとも１回誤り無く送ることのできる確率は、$1-(1-\eta)^{N}$である。

【０１４８】このＮ回の送出を分割数Ｋだけ繰り返したとき、Ｋ個の分割したバーストが全て少なくとも１回誤り無く送ることのできる確率は、

（２）

する場合では、最小０．６秒、最大１．２秒、図１３のフォーマットで２０４８ビット送受する場合では、最小５．１秒、最大１０．２秒となる。

【０１５２】また、通常のハードウェアで処理を行うＲＳＡ暗号を用いた認証の場合、認証を受ける側が上記のような認証用情報を生成するのに必要な計算処理の時間は、０．１～２秒程度である。

【０１５３】したがって、認証に伴う情報の送受と処理に要する時間は、合計すると０．７～１２．２秒程度となる。

【０１５４】この実施例に拠ると、送出回数が固定であるため、あらかじめ処理時間が算出できるという利点がある。これを生かすと、認証情報の処理と他の制御情報の処理とを並列処理する際にスケジューリングを用意に行うことができる。

【０１５５】また、図１１に示す実施例と比較して、比較的認証用情報の長さが短い場合に適しているといえる。

【０１５６】図１５に示す実施例では、暗号化情報の復号に伴う誤り検出機能を用いるものである。

【０１５７】認証にＲＳＡ暗号を用いる場合、暗号利用モードのうち、ＥＣＢ（Ｅｌｅｃｔｒｏｎｉｃ　Ｃｏｄｅ　Ｂｏｏｋ）モードとＣＢＣ（Ｃｉｐｈｅｒ　ＢｌｏｃｋＣｈａｉｎｉｎｇ）モードを用いることが考えられる。この二つのモードを利用した場合、伝送路上で１ビット誤った場合、復号側ではブロック全体、あるいはブロック全体および次のブロックにわたって誤りが波及する。

【０１５８】通常、暗号化する前のデータは、例えばＡＳＣＩＩコード表に従う、あるいは２進化１０進数を用いるなど、なんらかのフォーマットに従うようにされる。

【０１５９】したがって、ブロック全体に誤りが拡散した復号後のデータは、フォーマットに合わないことで、当該ブロックの伝送の際に誤りが発生したことを検出できる。　図１５は、ＥＣＢモードで、図１２に示すフォーマットを用いた場合の例を示す。認証方式としてＲＳＡ方式を考える場合、署名をして送り返すビット数は、５１２、１０２４の２通りが考えられる。ここでは５１２ビットを考えると、分割して送る場合に必要なバーストの数Ｋは３となる。これを連続して送信し、受信側では順次復号し、フォーマットに合うか否かを判断する。ここで、全てのバーストが送られてくるまで待つことなく、フォーマットに合うか否かを判断できる部分から判断をあらかじめ行うことで誤り発生検出を早い段階で行うことも考えられる。誤り発生を検出した場合には、認証を行う側に再送要求を出す。

【０１６０】また、無線端末ＰＳから基地局ＣＳへの認証用情報の送信には、ＣＲＣなどの誤り訂正ビットを設け、基地局ＣＳから無線端末ＰＳへの認証用情報の送信には、誤り訂正ビットを設けず、暗号の復号に伴う誤り検出機能を用いることも考えられる。

【０１６１】また上述の例とは逆に、基地局ＣＳから無線端末ＰＳへの認証用情報の送信には、ＣＲＣなどの誤り訂正ビットを設け、無線端末ＰＳから基地局ＣＳへの認証用情報の送信には、誤り訂正ビットを設けず、暗号の復号に伴う誤り検出機能を用いることも考えられる。

【０１６２】この実施例に拠ると、ＣＲＣなどの誤り検出専用のビットをバーストの中に設ける必要がなくなり、情報速度の向上、あるいは信号の狭帯域化が可能に＊なる。暗号専用の処理装置や高速の演算装置を用いると、認証処理と誤り検出が同時に非常に短時間で行うことができる。

【０１６３】

【発明の効果】以上述べたように本発明によれば、無線通信システムにおける無線端末の正当性確認と鍵共有を同時に、通信量少なく実現できる。また、無線端末と基地局相互の正当性確認と鍵共有を実現する場合にも、従来方式よりも通信量が少なくなる。

【図面の簡単な説明】

【図１】　無線端末の認証方式および無線端末と基地局の鍵共有方式の基本構成を表す図

【図２】　無線通信システムの構成図

【図３】　第１の実施例である無線端末の認証・鍵共有手順を示す図

【図４】　第２の実施例である無線端末の認証・鍵共有手順を示す図

【図５】　第２の実施例中の鍵共有関数の構成を示す図

【図６】　無線端末と基地局の相互認証方式と鍵共有方式の基本構成を表す図

【図７】　第３の実施例である無線端末と基地局の相互認証・鍵共有手順を示す図

【図８】　第４の実施例である無線端末と基地局の相互認証・鍵共有手順を示す図

【図９】　認証のシーケンスを示す図。

【図１０】　片方向のみの送受信を用いた認証のシーケンスを示す図。

【図１１】　認証用情報をバーストに分割し、自動再送手順を用いた場合の説明図。

【図１２】　バーストのフォーマット図

【図１３】　バーストのフォーマット図

【図１４】　認証用情報をバーストに分割し、複数回送信する場合の説明図。

【図１５】　暗号化情報の復号に誤り検出機能を用いる場合の説明図。

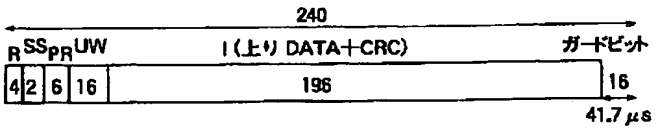
【符号の説明】

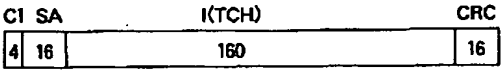
ＣＣ……制御局

ＣＳ……基地局

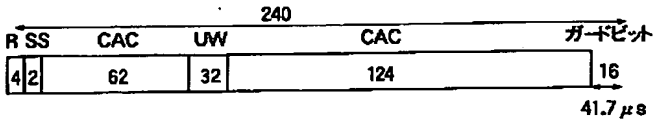
ＰＳ……無線端末

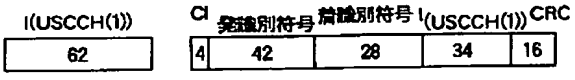
【図１２】



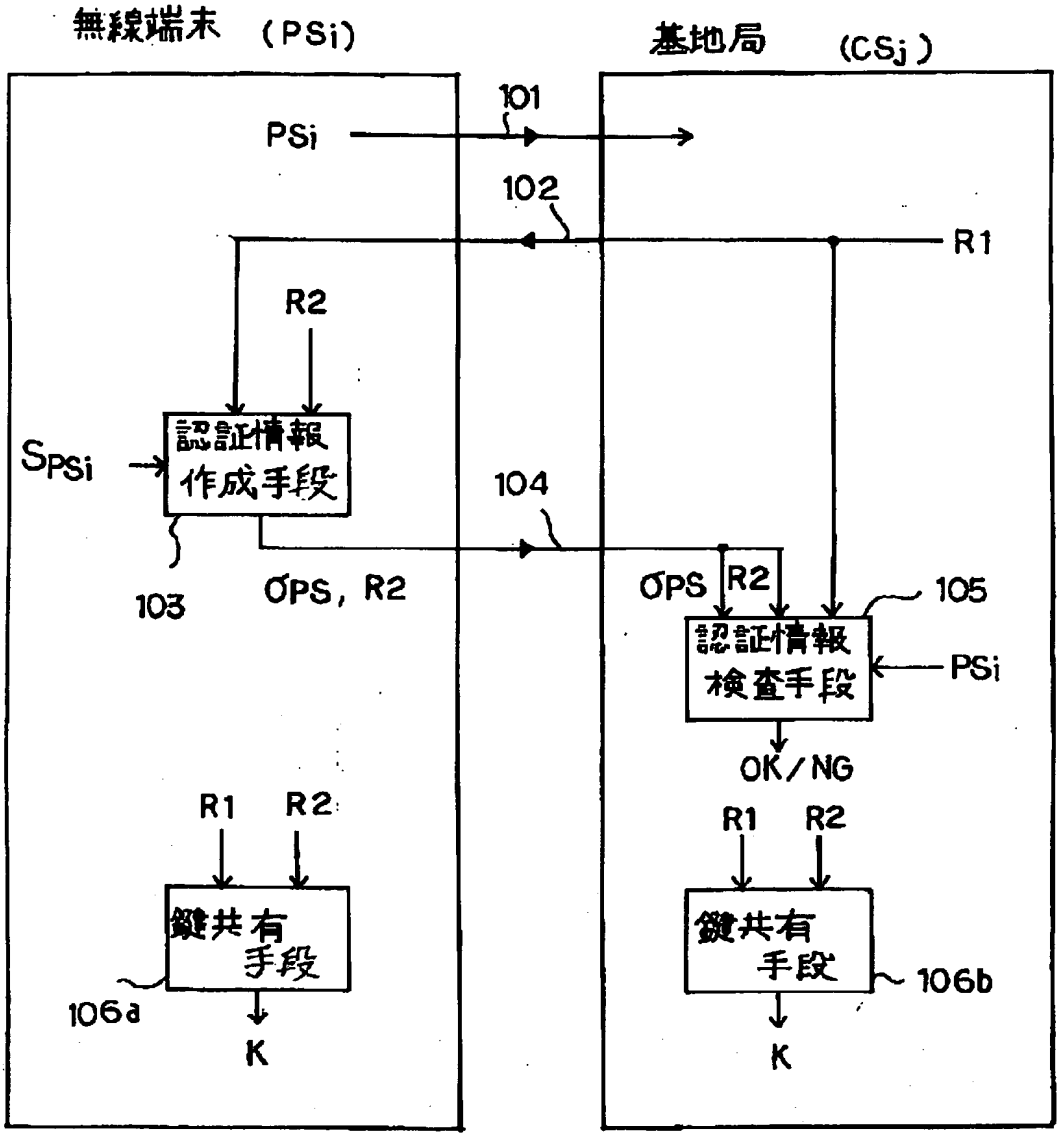


【図１３】

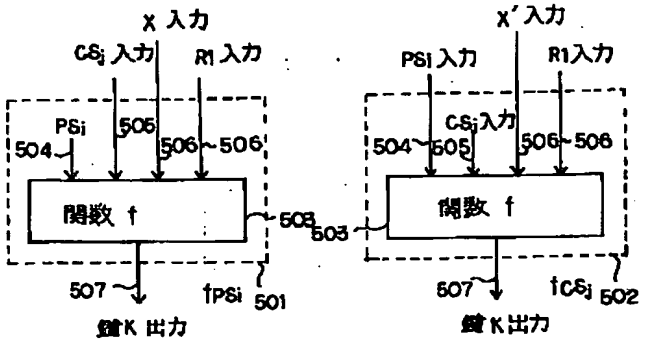




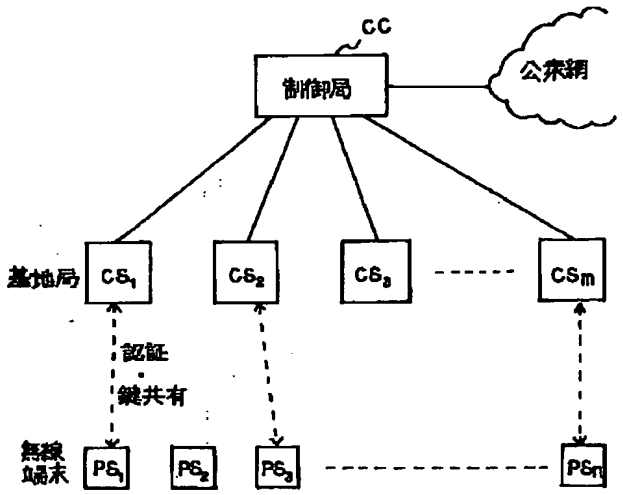
【図1】


無線端末 (PSi)
基地局 (CSj)
101
PSi
102
R1
R2
SPSi
認証情報作成手段
104
103
σPS, R2
σPS
R2
105
認証情報検査手段
PSi
OK/NG
R1
R2
R1
R2
鍵共有手段
106a
K
鍵共有手段
106b
K

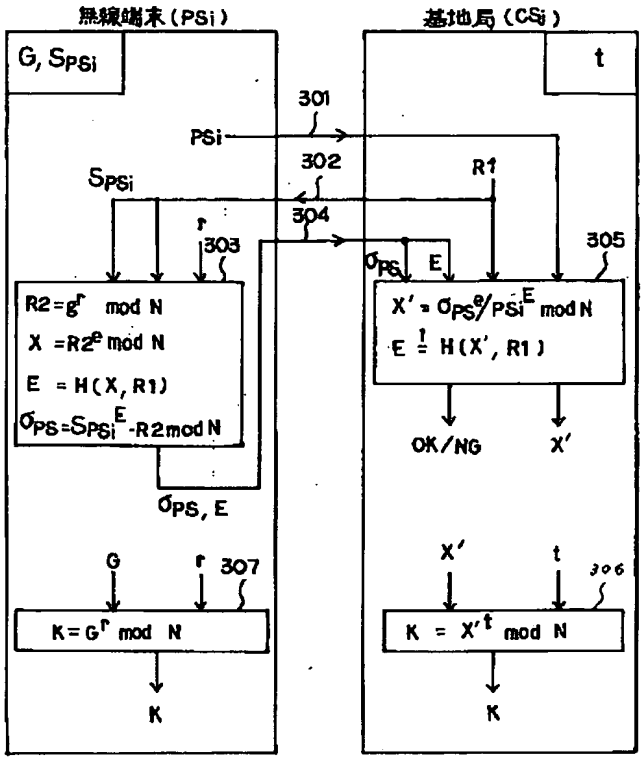
【図5】


X 入力
CSj 入力
R1 入力
PSi
504
505
506
506
506
関数 f
503
507
fPSi
501
鍵K出力
X' 入力
PSi 入力
R1入力
CSj入力
504
505
506
506
関数 f
503
507
fCSj
502
鍵K出力

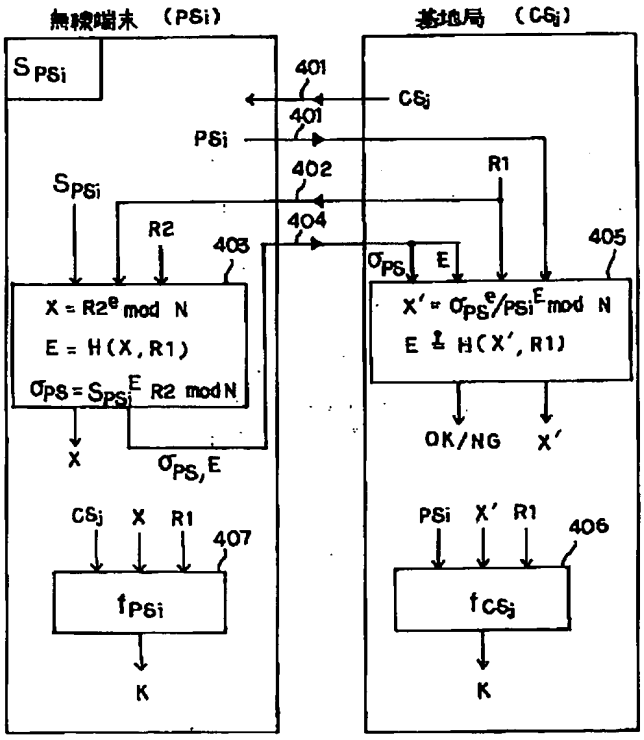
【図２】


CC
制御局
公衆網
基地局
CS1
CS2
CS3
CSm
認証
鍵共有
無線端末
PS1
PS2
PS3
PSn

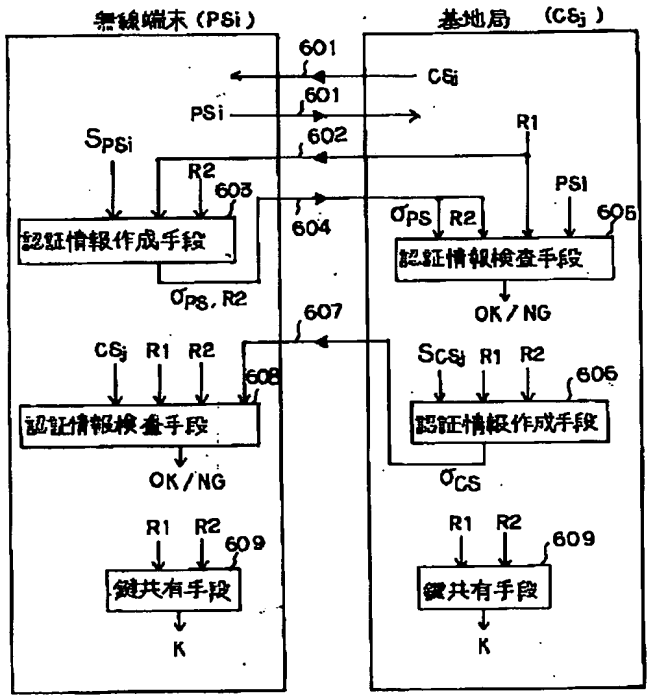
【図３】


無線端末（PSi）
基地局（CSj）
G, SPSi
t
301
PSi
302
SPSi
R1
304
r
303
305
R2=g^r mod N
X =R2^e mod N
E = H(X, R1)
σPS=SPSi^E・R2 mod N
σPS, E
X' = σPS^e/PSi^E mod N
E ? H(X', R1)
OK/NG
X'
G
r
307
X'
t
306
K = G^r mod N
K = X'^t mod N
K
K

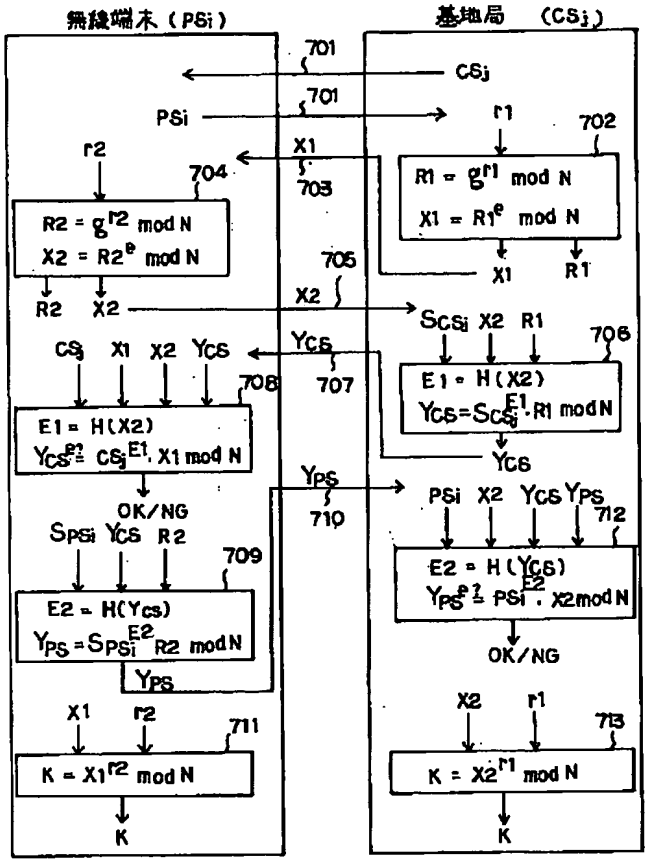
【図４】


無線端末 (PSi)
基地局 (CSj)
SPSi
401
CSj
401
PSi
402
SPSi
R1
404
R2
403
405
σPS
E
X = R2^e mod N
E = H(X, R1)
σPS = SPSi^E・R2 mod N
X' = σPS^e/PSi^E mod N
E ? H(X', R1)
OK/NG
X'
X
σPS, E
CSj
X
R1
407
PSi
X'
R1
406
fPSi
fCSj
K
K

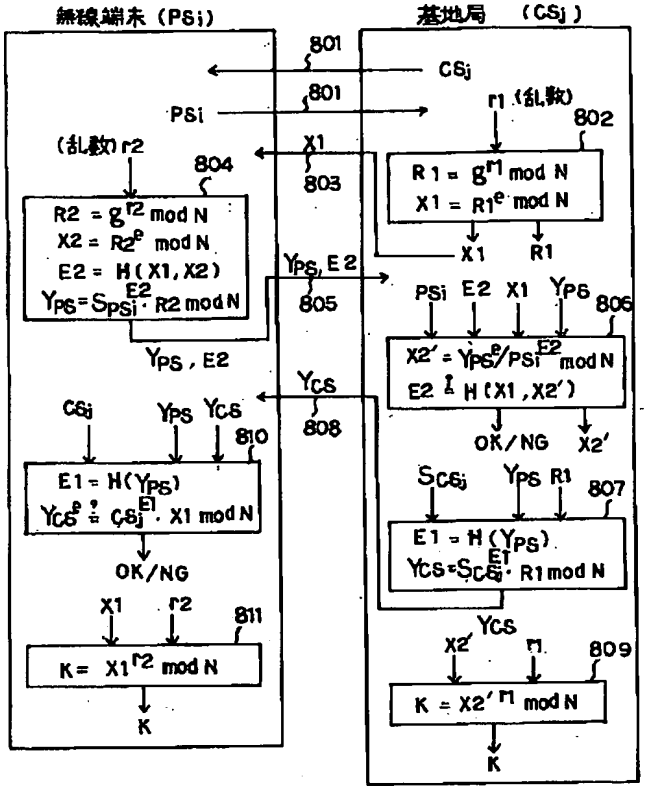
【図６】


無線端末 (PSi)
基地局 (CSj)
601
CSj
601
PSi
R1
602
SPSi
R2
603
PSi
σPS
R2
606
604
認証情報作成手段
認証情報検査手段
σPS, R2
OK/NG
607
CSj
R1
R2
608
SCSj
R1
R2
606
認証情報検査手段
認証情報作成手段
OK/NG
σCS
R1
R2
609
R1
R2
609
鍵共有手段
鍵共有手段
K
K

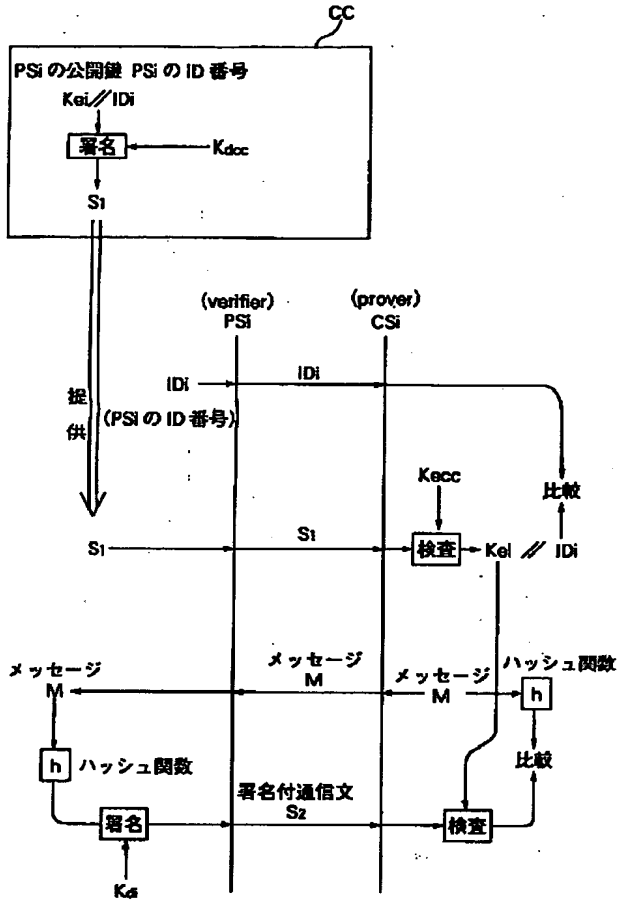
【図７】


無線端末（PSi）
基地局　（CSj）
701
CSj
PSi
701
r1
702
r2
X1
703
704
R1 = g^r1 mod N
X1 = R1^e mod N
R2 = g^r2 mod N
X2 = R2^e mod N
X1
R1
R2
X2
705
X2
SCSi X2 R1
706
CSj X1 X2 YCS
YCS
707
708
E1 = H(X2)
YCS = SCSi^E1 · R1 mod N
E1 = H(X2)
YCS = CSj^E1 · X1 mod N
YCS
OK/NG
YPS
710
PSi X2 YCS YPS
712
SPSi YCS R2
709
E2 = H(YCS)
YPS = SPSi^E2 R2 mod N
E2 = H(YCS)
YPS^E2 = PSi · X2 mod N
YPS
OK/NG
X1 r2
711
X2 r1
713
K = X1^r2 mod N
K = X2^r1 mod N
K
K

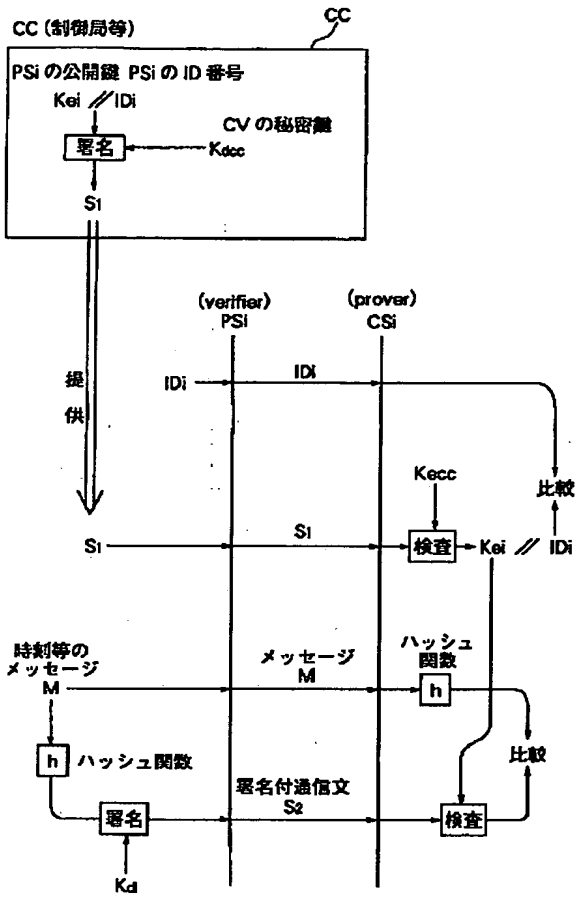
【図８】


無線端末（PSi）
基地局　（CSj）
801
CSj
801
r1 (乱数)
PSi
802
(乱数) r2
804
X1
803
R1 = g^r1 mod N
X1 = R1^e mod N
R2 = g^r2 mod N
X2 = R2^e mod N
E2 = H(X1, X2)
YPS = SPSi^E2 · R2 mod N
X1
R1
YPS, E2
805
PSi E2 X1 YPS
806
X2' = YPS^e / PSi^E2 mod N
E2 ≟ H(X1, X2')
YPS, E2
OK/NG
X2'
YCS
808
CSj YPS YCS
SCSj YPS R1
807
810
E1 = H(YPS)
YCS^e ≟ CSj^E1 · X1 mod N
E1 = H(YPS)
YCS = SCSj^E1 · R1 mod N
OK/NG
X1 r2
811
YCS
X2' r1
809
K = X1^r2 mod N
K = X2'^r1 mod N
K
K

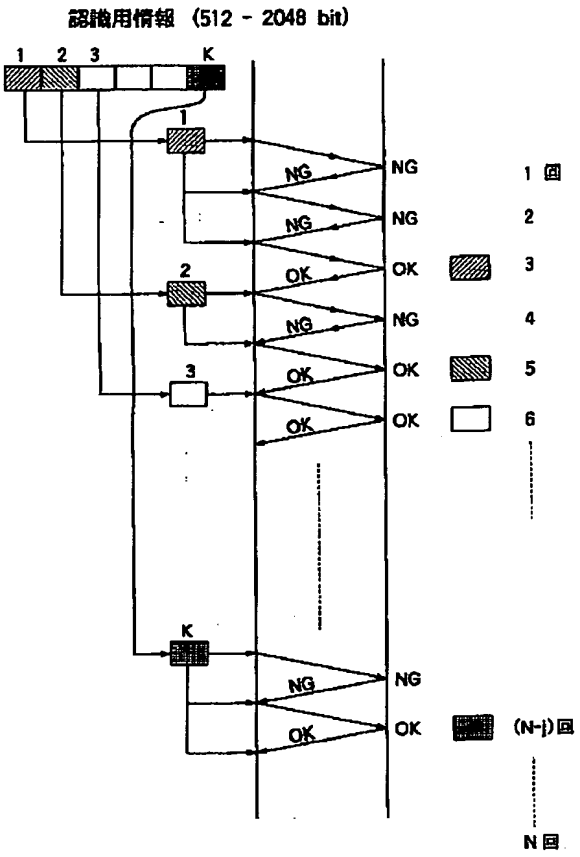
【図９】


CC
PSi の公開鍵 PSi の ID 番号
Kei // IDi
署名
Kdcc
Si
(verifier)
PSi
(prover)
CSi
提供
IDi
IDi
(PSi の ID 番号)
Kecc
比較
Si
Si
検査
Kei // IDi
メッセージ
M
メッセージ
M
メッセージ
M
ハッシュ関数
h
h
ハッシュ関数
比較
署名付通信文
S2
署名
検査
Kd

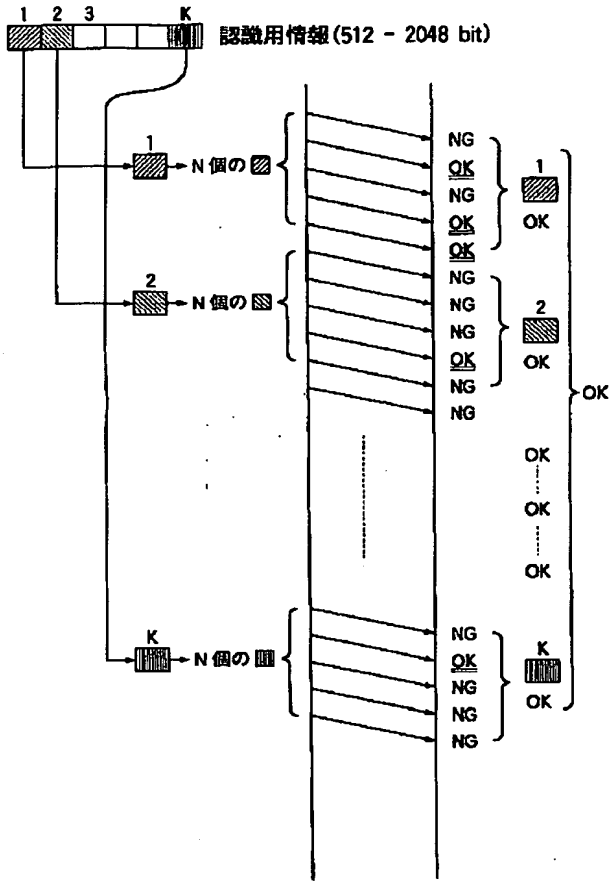
【図１０】


CC (制御局等)
CC
PSi の公開鍵 PSi の ID 番号
Kei // IDi
CV の秘密鍵
署名
Kdcc
Si
(verifier)
PSi
(prover)
CSi
提供
IDi
IDi
Kecc
比較
Si
Si
検査
Kei // IDi
時刻等の
メッセージ
M
メッセージ
M
ハッシュ
関数
h
h
ハッシュ関数
比較
署名付通信文
S2
署名
検査
Kd

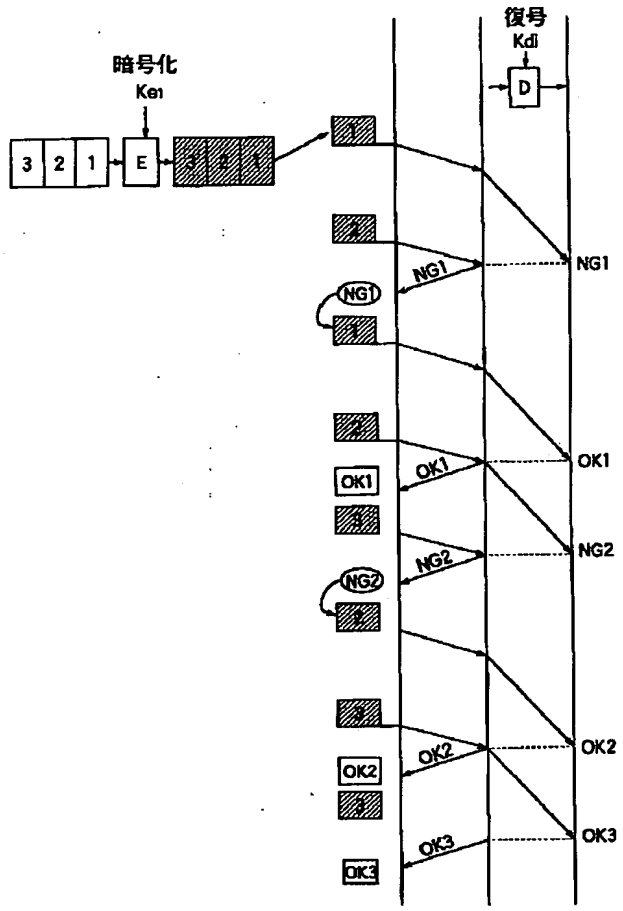
【図１１】


認識用情報 (512 - 2048 bit)
1 2 3 K
1
2
3
K
NG
NG
OK
NG
OK
OK
NG
OK
NG
OK
1 回
2
3
4
5
6
(N-j)回
N 回

【図１４】


1 2 3 K
認識用情報(512 - 2048 bit)
1
2
K
N 個の
N 個の
N 個の
NG
OK
NG
OK
OK
NG
NG
NG
OK
NG
NG
NG
OK
NG
OK
NG
NG
1
OK
2
OK
K
OK
OK
OK
OK
OK

【図１５】



フロントページの続き

(72)発明者　小倉　浩嗣
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝総合研究所内